

```
// pick a pseudo-random number between 0 and the number of WORDS (16-bit sets)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       // in the current ciphertext block and use it as this WORD pointer.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // PossibleChoices[FindBit] is the pseudo-random bit-location.
                                                                                                                                                // variable that will contain the index of the current assigned bit.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              AssignedBit=MRK. Value. c[(crc_mrk+BitPointer)%160]%AvailableBits; // pick a pseudo-random number between 0 and AvailableBits.
                                                                                                                                                                                             // index variable used for finding the assigned bit's position.
                                                                     // create empty array for keeping track of possible choices.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     // toop through possible tocations of the AssignedBit:
                                                                                                         // variable that will maintain a count of available bits.
                              // create empty array for keeping track of bit status.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  // mark bit as used so that it is not re-used.
                                                                                                                                                                                                                                                                                                                                                                                                                                     // increment the number of available bits.
                                                                                                                                                                                                                                 // obtain Master Recovery Key's CRC.
                                                                                                                                                                                                                                                                                                                                                                                                 // add it to the list of possibilities.
                                                                                                                                                                                                                                                                                                                                                             // if this bit is not already in use,
                                                                                                                                                                                                                                                                        // loop through 16 bit pointers:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      // if FindBit = AssignedBit,
                                                                                                                                                                                                                                                                                                                         // loop through useable bits:
int KeyGenerator::Locations(BitLocations& OrderedPairs, unsigned int CFB_Size)
                                                                                                                                                                                                                                                                                                                            for (AssignedBit=0, AvailableBits=0; AssignedBit<16; AssignedBit++)</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (MRK. Value.c[(crc_mrk+BitPointer)%160]%(CFB_Size/2))*2;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                OrderedPairs.Bit[BitPointer]=PossibleChoices[j];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 for (FindBit=0; FindBit<(AvailableBits+1); FindBit++)</pre>
                                       short BitStatus[16]={0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};
                                                                                                                                                                                                                                                                                                                                                                                                          PossibleChoices[AvailableBits]=AssignedBit;
                                                                                                                                                                                                                                                                                    for(short BitPointer=0;BitPointer<16;BitPointer++)</pre>
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 BitStatus[OrderedPairs.Bit[BitPointer]]=-1;
                                                                                                                                                                                                                                                                                                                                                                         if(BitStatus[AssignedBit]>-1)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        OrderedPairs.Word[BitPointer] =
                                                                                                                                                                                                                                                      unsigned char crc_mrk=MRK.CRC();
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if(FindBit==AssignedBit)
                                                                                                                                                                                                                                                                                                                                                                                                                                                    AvailableBits++;
                                                                                          short PossibleChoices[16];
                                                                                                                                 short AvailableBits;
                                                                                                                                                                           short AssignedBit;
                                                                                                                                                                                                                     short FindBit;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        return 1;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 20
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               25
                                                                                                                                                                        S
                                                                                                                                                                                                                                                                                                                                                                            10
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   15
```

Table 1 Generation of the ECD Code and Insertion Into Ciphertext Block